Lecture -1

Question 1. When is a subgroup K called normal?

Answer. if $gK = Kg$ for all $g \in G$.

Question 2. Define a permutation on the set X.

Answer. A bijection

$$f : X \to X$$

Question 3. What does it mean that $sgn(S_n)$ is well defined?

Answer. If

$$\sigma = \tau_1 \ldots \tau_a$$
$$= \tau_1' \ldots \tau_b'$$

then $(-1)^a = (-1)^b$.

Question 4. How do we denote the set of all permutations of X?

Answer. Sym(X)

Question 5. Sketch a geometric proof that the group D_{2n} is $\{e, r, r^2, \ldots, r^{n-1}, t, rt, \ldots, r^{n-1}t\}$ under composition.

Answer. Let f be a symmetry of P f(1) maps to another vertex of P (say k). Let g be the rotation of f such that f(1) = 1. The vertex adjascent to 1 is either fixed or reflected. If it is fixed, g is the identity, meaning f is a rotation. Otherwise, g is a reflection then a rotation.

Question 6. State the Fermat-Euler Theorem

Answer. Let $a \in \mathbb{N}, n \in \mathbb{Z}, (a, n) = 1$.

$$a^{\phi(n)} \equiv 1 \mod n$$

Question 7. Show a k-cycle can be written as a product of transpositions

Answer. $(a_1, a_2, \ldots, a_n) = (a_1, a_2)(a_2, a_3), \ldots (a_{k-2}, a_{k-1})(a_{k-1}, a_k)$.

Question 8. What is the index of H in G denoted $|G : H|$?

Answer. It is the number of left cosets of H in G.

Question 9. Define (informally) a k-cycle

Answer. $\sigma = (a_1, a_2, \ldots, a_k)$, mapping a_1 to a_2, a_2 to $a_3, \ldots, a_k$ to a_1. It leaves all other elements of S_n fixed.

Question 10. When is a group H cyclic?

Answer. If there exists an element h in H such that each element of H is a power of h.

Question 11. When is a group H cyclic?

Answer. If there exists an element h in H such that each element of H is a power of h.

Question 12. Let $H \leq G$, $a, b \in G$. Prove
$a^{-1}b \in H \Rightarrow aH = bH$

Answer. Suppose $a^{-1}b = k \in H$
$b = ak \in aH$
also $b \in bH$
So $aH = bH$.

Question 13. What is a coset of G?

Answer. Let $H \leq G$, and $g \in G$. The left coset gH is defined to be

$$\{gh : h \in H\}$$

, similar for right coset.

Question 14. Sketch a proof of the claim that the map

$$\mathrm{sgn}(S_n, \circ) \to (\{\pm 1\}, \times)$$

is a homomorphism (assuming well-defined and non-trivial)

Answer. Suppose $a, b \in S_n$ Writing out a,b as transpositions it follows that sgn(ab) = sgn(a)sgn(b).

Question 15. How do we generate a minimal cycle of a permutation sigma?

Answer. $a_1 \in \{1, 2, \ldots, n\} = X$
Consider $a_1, \sigma(a_1), \sigma^2(a_1), \ldots$
Since X is finite, $\exists$ minimal j s.t. $\sigma^j(a_i) \in \{a_1, \sigma(a_1), \ldots, \sigma^{j-1}(a_1)\}$

Claim: $\sigma^j(a_1) = a_1$.
Since if not,
$\sigma^j(a_1) = \sigma^i(a_i)$ for $j > i \geq 1$
$\sigma^{j-i}(a_1) = a_1$ contradicting minimality of j.

Question 16. Define (formally) a k-cycle

Answer. Let $a_1, \dots a_k$ be distinct integers in $\{1, \dots n\}$. Suppose $\sigma \in S_n$ and

$$\sigma(a_i) = a_{i+1}$$
$$\sigma(a_k) = a_1$$

for $1 \leq i \leq k-1$, and $\sigma(x) = x, \ \forall x\{1, \dots, n\}/\{a_1, \dots, a_n\}$.

Question 17. How do we algebraically write D_{2n}?

Answer.

$$D_{2n} =< r, t | r^n = e, t^2 = e, trt = r^{-1} >$$

Question 18. Let $(G, \star_G), (H, \star_H)$ be groups. When is

$$\theta : G \to H$$

a homomorphism?

Answer.

$$\theta(x \star_G y) = \theta(x) \star_H \theta(y)$$
$$\forall x, y \in G$$

Question 19. Prove the image of $\theta(G) : G \to H$ is a subgroup of H

Answer. NEED TO CHECK LECTURE NOTES

Question 20. Let $\theta : G \to H$ be a homomorphism. What is the image of θ?

Answer. $\theta(G) = \{\theta(g) : g \in G\}$

Question 21. Prove that if aH n bH isn't empty, then aH = bH.

Answer. Let c be an element in the intersection. $c = ak$ for some k in H, by writing set definition of cH we see that cH is a improper subset of aH.

Similarly, $a = ck^{-1}$, which is an element of cH
So aH is a improper subset of cH.
So $aH = cH$. Similarly $cH = bH$ so $aH = bH$.

Question 22. From what lemma does the existence of the alternating group A_n follow from?

Answer. The map

$$\text{sgn}(S_n, \circ) \to (\{\pm 1\}, \times)$$

is a well-defined and non-trivial homomorphism.

Question 23. Sketch a proof that the function

sgn: $S_n \to \{\pm 1\}$ $\sigma \to \text{sgn}(\sigma)$

is well-defined.

Answer. Given $\tau = (a, b)$ is a transposition, we show $\sigma\tau \mod 2 \cong \sigma + 1$ by considering the two cases: a and b are in the same cycle, and a and b are in distinct cycles.
In both cases we can rewrite the product of cycles such that the claim holds.
We know c(identity) = n, so assuming σ has two decompositions, we can show a = b mod 2, from which claim holds.

Question 24. Sketch a group-theoretic proof of the Fermat-Euler theorem

Answer. $R_n = \{1, \ldots, n-1\}$
Let $R_n^* = \{a \in R_n : (a, n) = 1\}$
$(R_n^*, \times_n)$ is a group

so claim follows from Lagrange.

Question 25. What is $GL_2(R)$?

Answer. The group of all 2x2 matrices with non-zero determinants under multiplication

Question 26. Prove Sym(X) is a group under composition.

Answer. *closure - composition of bijections forms a bijection
*identity, define $c(x) = x$ for all x in X
*inverse - $f \in Sym(X)$, since f is a bijection, f^{-1} exists and is a bijection, satisfying $f^{-1} \circ f = e = f^{-1} \circ f$
*associativity - composition of functions is associative

Question 27. Sketch a proof for the uniqueness of inverses

Answer. Suppose y,z are inverses of x. y = y*e = y*(x*z) and use associativity to show y = z.

Motivation: think about this fact is contingent on - if associativity didn't hold, it'd make sense for there to exist a left inverse and a right inverse. Therefore, we want to try and sneak associativity into this. The only way we can do this is by introducing three terms.

Question 28. What is the symmetric group of degree n?

Answer.

$$S_n = Sym(\{1, 2, \ldots, n\})$$

the set of all permutations of $\{1, 2, \ldots, n\}$.

Question 29. How do we define a rotation r in D_{2n}?

Answer.

$$r : P \mapsto P$$
$$z \mapsto e^{2\pi i/n} z$$

Question 30. Let $H \leq G$, $a, b \in G$. Prove $aH = bH \to a^{-1}b \in H$

Answer. $b \in bH = aH$ $b = ah$ for some h inH $a^{-1}b = h \in H$

Question 31. Define a binary operation

Answer. A binary operation * on a set X is a way of combining two elements of X to give another element of X.

Question 32. Prove that the inverse of $a \in R_n^*$ is in R_n^*

Answer. Claim follows from Bezout on (a,n)=1 and rearranging.

Question 33. Sketch a proof of Lagranges corollary.

Answer. Apply Lagranges theorem to the subgroup ¡g¿ of G.

Question 34. State Lagranges corollary

Answer. G is a finite group and $g \in G$. Then $o(g)\big||G|$. In particular, $g^{|G|} = e$.

Question 35. Prove Lagrange's theorem.

Answer. G is partitioned into k distinct cosets of H. Each coset is the same size. So $|G| = |H|$ k.

Question 36. Sketch a proof of the claim that the map

$$\mathrm{sgn}(S_n, \circ) \to (\{\pm 1\}, \times)$$

is a well-defined and non-trivial

Answer. - Well defined since $sgn(S_n)$ is well defined. - $sgn((1,2)) = -1$, so non-trivial. (not just equal to identity)

Question 37. Suppose (k,l) are in the same cycle within σ. How do we "factor" $\sigma(k,l)$ into disjoint cycles?

Answer.

$$(k, a_1, \ldots, a_r, l, b_1, \ldots, b_s)(k, l)$$
$$(k, b_1, \ldots, b_s)(l, a_1, \ldots, a_r)$$

Question 38. Suppose (k,l) are in different cycles of σ. How do we "factor" $\sigma(k,l)$ into disjoint cycles?

Answer.

$$(k, a_1, \ldots, a_r)(l, b_1, \ldots, b_s)(k, l)$$
$$= (k, b_1, b_2, \ldots, b_s, l_1, a_2, \ldots, a_r)$$

Question 39. How do we define a reflection t in $D_2 n$?

Answer.

Question 40. Prove the only subset of Z under addition is nZ

Answer. If $H = \{0\} = 0\mathbb{Z}$

Otherwise, choose $0 < n \in H$ with n minimal. $n\mathbb{Z} \subseteq H$ by closure and inverses. We show $H = n\mathbb{Z}$. Suppose $\exists h \in H \setminus n\mathbb{Z}$, can write $h = nk + h'$, with $h' \in \{1, 2, \ldots, n-1\}$

But $h' = h - nk \in H$, contradicting minimality of n. Thus $H = n\mathbb{Z}$

Question 41. Show that the identity element is unique

Answer. Formally state what it means for e and $\hat{e}$ to be identities and show that this implies they are equal.

Question 42. What is $|G : H|$ for finite G,H in terms of the order of G and H?

Answer. $|G : H| = |G|/|H|$.

Question 43. What does Lagrange's Theorem state?

Answer. Let H be a subgroup of the finite group G. Then the order of H divides the order of G.

Question 44. Let σ, τ be disjoint cycles in S_n. Prove $o(\sigma\tau) = \text{lcm}(o(\sigma), o(\tau))$

Answer. ($\Leftarrow$)verify, recall σ and τ commute because disjoint
($\Rightarrow$) Suppose $o(\tau\sigma) = n$,

$$(\sigma\tau)^n = e$$
$$\sigma^n\tau^n = e$$

But σ, τ move different elements of X,
So $\sigma^n = e$, $\tau^n = e$
So $o(\sigma)|n$ and $o(\tau)|n$
So $k = \text{lcm}(o(\sigma), o(\tau))$

Question 45. What must hold for (G, *) to be a group?

Answer. (i) Identity exists (ii) Inverse exists (ii) (x*y)*z = x*(y*z)

Question 46. What is $SL_2(R)$? (special linear)

Answer. The set of all 2x2 matrices with determinant 1 under multiplication

Question 47. (Sketch) proof that $K \trianglelefteq G$ means $G\ K$ exists

Answer. Check coset multiplication is well defined, ie. that two cosets multiplied always give the same result (this ¡=¿ normal). Verify closure, identity and inverse.

Question 48. What is the first isomorphism theorem?

Answer. Let G, H be groups and

$$\theta : G \to H$$

a group homomorphism. Then $Im\theta \leq H$, $Ker\Theta \trianglelefteq G$
and $G \backslash Ker\theta \cong Im\theta$

Question 49. What is the first isomorphism theorem?

Answer. Let G, H be groups and

$$\theta : G \to H$$

a group homomorphism. Then $Im\theta \leq H$, $Ker\Theta \trianglelefteq G$
and $G \backslash Ker\theta \cong Im\theta$

Lecture 10

Question 50. What is a simple group?

Answer. A group with no non-trivial subgroup.

Question 51. Prove the 1st isomorphism theorem

Answer. Construct an isomorphism ϕ

$$G \backslash \text{Ker}\theta \to \text{Im}\theta$$

Let $K = \text{Ker}\theta$,

$$gK \to \theta(g)$$

Prove ϕ is well-defined, homomorphism and bijection.

Question 52. Prove that a homomorphism $\theta : G \to H$ is injective iff

$$\text{Ker}\theta = \{e\}$$

Answer. Consider both directions to show it is injective.

Lecture 11

Question 53. Let G be a group with subgroups H and K.

Answer. Consider both directions to show it is injective.

Question 54. Prove that if,
(i) each elem of G can be written as hk ($h \in H$, $k \in K$)
(ii) $H \cap K = \{e\}$
(iii) $hk = kh \forall k \in K, h \in H$,
then
$G \cong H \times K$

Answer. Show the map

$$\theta : H \times K \to G$$
$$\theta(h, k) \to hk$$

is an isomorphism.

Question 55. There are alternate, equivalent definitions of internal direct product.
Show that
(i) each elem of G can be written as hk ($h \in H$, $k \in K$)
(ii) $H \cap K = \{e\}$
(iii) $hk = kh \forall k \in K, h \in H$,
is equivalent to (i)' $H \trianglelefteq G, K \trianglelefteq G$ (ii)' $H \cap K = \{e\}$
(iii) HK = G.

Answer. $\Rightarrow$ use (iii) to show (i)' and (i) implies (iii)'
$\Leftarrow$ Use (i)' to show (iii), (i) immediate from (iii)

Lecture 12

Question 56. Classify groups of order 6 up to isomorphism.

Answer. Consider order of elements with lagrange. if $o(g) = 6$, then $G \cong C_6$.
Can't have all elems order 2, since $|G|$ isn't a power of two.
We always have an element a of order 3. (g^2 if o(g) = 6).
Consider $b \in G \backslash \langle a \rangle$; $b^2 \in \langle a \rangle$
$bab^{-1} \in \langle a \rangle$ and consider cases.

Question 57. Classify groups of order 8 up to isomorphism

Answer. If all elems order 2, then we have $C_2 \times C_2 \times C_2$. Prove by quotienting out
If an elem has order 8, then C_8.
Let a have order 4. Consider $b \in G \backslash \langle a \rangle$.
$b^2 \in \langle a \rangle$
If $b^2 = a$ or a^3, then $o(b) = 8$, so C_8.

Consider $bab^{-1} = a^i$, and evaluate b^2ab^{-2} in two ways to show $i = \pm 1$.
Consider the four cases in i and b^2 to get groups.

Lecture 13

Question 58. Define a group action ϕ.

Answer. G acts on X with the map
$\phi : G \times X \to X$
$(g, x) \to \phi(g, x) = g(x)$
such that
(1) closure (implied by notation) (2) gh(x) = g(h(x)) (3) identity acting on x is sent to x

Lecture 14

Question 59. Define a group action in terms of Sym(X)

Answer. If G is a group and X is a set such that

$$\Phi : G \to \text{Sym}(X)$$

is a group homomorphism, then

$$\phi : G \times X \to X$$

$$(g, x) \to \phi_g(x)$$

where $\Phi(g) = \phi_g$, is a group action.

Question 60. What is a faithful action?

Answer. Ker$\Phi = \{e\}$; the only x acted to the identity is the identity.

Question 61. What does Cayley's theorem state?

Answer. Every group is isomorphic to a subgroup of Sym(X) for some X.

Question 62. Prove Cayley's theorem

Answer. Consider the left regular action.

$$\Phi : G \times G \to G$$

$$(g, h) \to gh$$

This action is faithful (show), so we have an injective homomorphism

$$\Phi : G \to \text{Sym}(G)$$

So $G \cong \text{Im}\Phi \leq \text{Sym}(G)$ as required.

Question 63. Define the orbit of $x \in X$

Answer.

$$\mathrm{Orb}_G(x) = \{g(x) : g \in G\} \subseteq X$$

The orbit of x is the set of points in X that it can map to.

Lecture 15

Question 64. Define a transitive action

Answer. G acts transitively on X if for any $x \in X$, $\mathrm{Orb}_G(x) = X$.

Question 65. Prove the distinct G-orbits form a partition of X.

Answer. Suppose $z \in \mathrm{Orb}_G(x) \cap \mathrm{Orb}_G(y)$.
Show $\mathrm{Orb}_G(x) = \mathrm{Orb}_G(z) = \mathrm{Orb}_G(y)$.

Question 66. Show that $\mathrm{Orb}_G(x)$ is invariant, i.e.

$$g(\mathrm{Orb}_G(x)) \subseteq \mathrm{Orb}_G(x).$$

Answer. just do it

Question 67. Show that G is transitive on $\mathrm{Orb}_G(x)$

Answer. this means any element in $\mathrm{Orb}_G(x)$ can go to any other element in $\mathrm{Orb}_G(x)$. construct this

Question 68. Define the stabilizer of x in G

Answer. $\mathrm{Stab}_G(x) = \{g \in G : g(x) = x\}$

Question 69. Prove $\mathrm{Stab}_G(x)$ is a subgroup of G.

Answer. just do it

Question 70. Prove the orbit-stabilizer theorem.

Answer. We prove that the index of $\mathrm{Stab}_G(x)$ is $|\mathrm{Orb}_G(x)|$.
Consider the map

$$\theta : \mathrm{Orb}_G(x) \to (G : \mathrm{Stab}_G(x))$$

$$g(x) \to g\mathrm{Stab}_G(x)$$

Now prove this is a well-defined bijection.

Lecture 16

miao

Lecture 17

Question 71. State Cauchy's theorem.

Answer. Let G be a finite group and p a prime that divides $|G|$. Then there exists an element in G of order p.

Question 72. Prove Cauchy's theorem.

Answer.

$$X = \{(x_1, x_2, \dots, x_p) : x_1 x_2 \cdots x_p = e, x_i \in G\}$$

Let $H = \{h : h^p = e\} \cong C_p$ which acts on X as follows

$$H \times X \to X$$

$$(h, (x_1, \dots, x_p)) \to (x_2, x_3, \dots, x_p, x_1)$$

In general

$$(h^i, (x_1, x_2, \dots, x_p)) \to (x_{1+i}, x_{2+i}, \dots, x_{p+i})$$

With suffix k taken $(k - 1 \mod p) + 1$.
Check this is a group action. Using the fact $|\text{Orb}_H(\bar{x})| = 1$ or p (by O/S), that

$$p \,\Big|\, \sum_{\text{distinct orbits}} \text{Orb}_H(\bar{x}),$$

and that

$$\text{Orb}_H(e, e, \dots e)) = 1$$

to show that $\bar{x} \neq e$ exists such that

$$\text{Orb}_H(\bar{x}) = 1,\ \bar{x} = (x, x, \dots x)$$

meaning $x^n = e$.

Question 73. What is the conjugacy action?

Answer.

$$G \times G \to G$$

$$(g, h) \to ghg^{-1}$$

Question 74. Given $z \in Z(G)$, what is $\text{ccl}_G(z)$?

Answer. 1

Question 75. Write $Z(G)$ in terms of the centralizers in G.

Answer. $Z(G) = \bigcap_{h \in G} C_G(h)$

Question 76. How can we relate the order of two elements in the same conjugacy class

Answer. They are equal

Question 77. What is the orbit and stabilizer of the conjugacy action?
Answer. The orbit are conjugacy classes and the stabilizers are called centralizers.

Question 78. Prove that if $|G| = p^n$ for some prime p, then $Z(G)$ is non-trivial.
Answer.

$$G = \bigcup_{\text{distinct conj classes}} \mathrm{ccl}_G(x)$$

By Orbit-Stabilizer theorem, $\mathrm{ccl}_G(x) \mid |G| = p^n$
So $|\mathrm{ccl}_G(x)| = 1$ or $p \mid |\mathrm{ccl}_G(x)|$
But

$$|G| = \sum_{x \in Z(G)} \mathrm{ccl}_G(x) + \sum_{\text{distinct classes w/}p \mid \mathrm{ccl}_G(x)} \mathrm{ccl}_G(x)$$

So

$$p \mid \sum_{x \in Z(G)} \mathrm{ccl}_G(x) = Z(G)$$

so $|Z(G)| > 1$.

Question 79. Prove that if $G \backslash Z(G)$ is cyclic, then G is abelian.
Answer. just do it lolololol

Lecture 18

Question 80. Prove that if $G \backslash Z(G)$ is cyclic, then G is abelian.
Answer. just do it lolololol

Question 81. Let $\sigma \in S_n$. Define the cycle type of σ.
Answer. σ can be written as a product of disjoint cycles including 1-cycles. Then the cycle type of σ is $(n_1, n_2, \dots, n_k)$ where $n_1 \leq n_2 \cdots \leq n_k$ and the ith cycle of σ has length n_i

Question 82. Prove that π and σ are conjugate in S_n iff they have the same cycle type.
Answer. σ can be written as a product of disjoint cycles including 1-cycles. Then the cycle type of σ is $(n_1, n_2, \dots, n_k)$ where $n_1 \leq n_2 \cdots \leq n_k$ and the ith cycle of σ has length n_i.
Consider τ conjugating σ, and consider the (general!) element $\sigma(a_{ij})$ and unwrap notation until you can write a product of disjoint cycles for the conjugation.

To show the converse, write π similarly to σ but with b_{ij} and then show, with $\tau(a_{ij}) = b_{ij}$, that $\pi = \tau\sigma\tau^{-1}$.

Question 83. Let $x \in A_n$. If $\mathrm{C}_{A_n}(x) = \mathrm{C}_{S_n}(x)$, how can we relate the size of $\mathrm{cl}_{A_n}(x)$ and $\mathrm{ccl}_{S_n}(x)$?

Answer.

$$|\mathrm{ccl}_{A_n}(x)| = \frac{|\mathrm{ccl}_{S_n}(x)|}{2}$$

Question 84. Let $x \in A_n$. If $\mathrm{C}_{A_n}(x) \nleq \mathrm{C}_{S_n}(x)$, how can we relate the size of $\mathrm{cl}_{A_n}(x)$ and $\mathrm{ccl}_{S_n}(x)$?

Answer.

$$|\mathrm{ccl}_{A_n}(x)| = |\mathrm{ccl}_{S_n}(x)|$$

Lecture 19

Question 85. What are the number of elements in S_n with k_L cycles of length L?

Answer.

$$\frac{n!}{\prod_L k_L! L^{k_L}}$$

Question 86. Prove A_5 is a simple group.

Answer. Suppose $N \trianglelefteq A_5$. Then N is a union of conjugacy classes.
$\Rightarrow |N| = 1 + 15a + 20b + 12c$ where $a, b \in \{0, 1\}, c \in \{0, 1, 2\}$.
But by Lagrange, $|N| \big| |A_5| = 60$.
Only possibility is $|N| = 1$ or 60.

Question 87. Prove $\mathrm{GL}_n(\mathbb{R})$ is a group under matrix multiplication.

Answer. closure, identity, inverse: don't be noob associative: use index notation

Question 88. Prove

$$\mathrm{Det} : \mathrm{GL}_n(\mathbb{R}) \to (\mathbb{R} = ckslash\{0\}, \times)$$

$$A \to \mathrm{det} A$$

is a surjective homomorphism

Answer. do it

Question 89. What is $\mathbb{F}_p$?

Answer. It is the finite field

$$\mathbb{F}_p = (\{0, 1, \ldots, p-1\}, +_p, \times_p).$$

Lecture 20

Question 90. What is $|GL_3(\mathbb{F}_p)|$?

Answer. Consider no. choices for each column.
Column 1: $p^3 - 1$
Column 2: $p^3 - p$
Column 3: $p^3 - p^2$

Question 91. What is $O(\mathbb{R})$

Answer. Orthonormal group.

$$\mathrm{O}_n(\mathbb{R}) = \{A \in M_n : AA^T = I\}$$

Lecture 21

Question 92. Prove $O(\mathbb{R})$ is a group

Answer. :3

Question 93. Let $A \in \mathrm{O}_n(\mathbb{R})$ and $\mathbf{x}, \mathbf{y} \in M_n$, then
(i) $A\mathbf{x} \cdot A\mathbf{y} = \mathbf{x} \cdot \mathbf{y}$
(ii) $|Ax| = |x|$ So A is an isometry.

Answer. Start from givens and unravel definitions.